



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/575,650	03/05/2007	Peter Bennett	851963.424USPC	2255
38106 7590 02/02/2010 SEED INTELLECTUAL PROPERTY LAW GROUP PLLC 701 FIFTH AVENUE, SUITE 5400 SEATTLE, WA 98104-7092				
EXAMINER ABRISHAMKAR, KAVEH				
ART UNIT 2431		PAPER NUMBER		
MAIL DATE 02/02/2010		DELIVERY MODE PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/575,650

Applicant(s)

BENNETT ET AL.

Examiner

KAVEH ABRISHAMKAR

Art Unit

2431

Period for Reply -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 October 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 24-29 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-18, and 24-29 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/GS/US)
Paper No(s)/Mail Date _____

- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment received on October 5, 2009. Claims 1-18, and 24-29 are currently pending consideration.

Response to Arguments

Applicant's arguments filed October 5, 2009 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Art (CPA), Bowman (U.S. Patent 5,999,623) in view of Johnson (U.S. Patent 7,143,294), does not teach a decrypting an encrypted enable signal in accordance with a pre-stored key on the integrated circuit. This argument is not found persuasive. Bowman states that in one embodiment, the KG algorithm is performed before the encryption information is received and stored until the encrypted information is received and then when the encrypted information is received, the decryption key is forwarded to the decryption unit (Bowman: column 7, lines 35-55). The decryption key (d-key) which is forwarded, its pre-stored in memory locations (Bowman: column 8, lines 20-30). Therefore, it is asserted that the key value is pre-stored, and the arguments are not found persuasive.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bowman et al. (U.S. Patent 5,999,623) in view of Johnson (U.S. Patent 7,143,294).

Regarding claim 1, Bowman discloses:

A semiconductor integrated circuit for use in an audio-video device arranged to produce audio-video signals, comprising:

an input interface for receipt of a received encrypted enable signal (column 2, lines 26-30: *authorized receiver receives an encrypted signal*);

an output interface for output of audio-video signals (Fig. 4b: *step AJ: outputs decrypted information*);

one or more hardware circuit portions each arranged to process data in relation to the audio-video signals (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*);

a decryption circuit arranged to receive the encrypted enable signal and to decrypt the encrypted enable signal in accordance with a key to provide a plain text message (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*);

a store containing a stored value for the circuit (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*);

a second decryption circuit in one or more hardware circuit portions and arranged to receive a common key from a common key store in the integrated circuit and to decrypt the received encrypted broadcast signal in response to receipt of the common key and the generation of the enable signal (column 6, lines 40-55: *wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly teach an enabling circuit to selectively restrict, deny or allow operation of a hardware circuit portion and a comparison circuit to compare the plain text message to the stored value to instruct the enabling device. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit comprises one or more switch elements arranged to selectively interrupt a data pathway to, from, or within at least one of the one or more of the hardware circuit portions (Johnson: column 6, lines 10-20: *enabling circuit*).

Claim 3 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the data pathway is a critical data pathway, whereby interruption of the pathway prevents operation of the at least one of the one or more hardware circuit portions (Johnson: column 6, lines 10-42).

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the data pathway relates to a clock of one or more hardware circuit portions, whereby interruption of the data pathway causes the clock to run slower than normal (Johnson: column 6, lines 10-42).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 4 wherein the one of the one or more hardware circuit portions is a main CPU of the semiconductor integrated circuit (column 6, lines 10-42).

Claim 6 is rejected as applied above in rejecting claim 5. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions is a display engine, whereby interruption of the data pathway causes the video signals at the output interface to be interrupted or impaired (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 7 is rejected as applied above in rejecting claim 2. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions is a data port of the semiconductor integrated circuit, whereby interruption of the data pathway prevents operation of the data port (column 6, lines 10-42).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from a broadcast signal (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from a manual input device (Fig. 4b: step AJ: *outputs decrypted information*).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the input interface is arranged to receive the encrypted enable signal from another device (column 6, lines 10-42: *signal received from the comparator device*).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit comprises a store arranged to store indications of hardware circuit elements to be restricted, denied, or allowed to operate (column 6, lines 10-42).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 11 wherein the store comprises one or more hardware fuses (column 6, lines 10-42).

Claim 13 is rejected as applied above in rejecting claim 11. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 11 wherein the store comprises a non-volatile memory (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Johnson discloses:

The semiconductor integrated circuit according to claim 1 wherein the enabling circuit is arranged to extract from the plain text message indications of which hardware circuit elements should be restricted, denied, or allowed to operate (column 6, lines 10-42).

Claim 15 is rejected as applied above in rejecting claim 1. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 1 wherein the semiconductor integrated circuit is a monolithic circuit for decryption of broadcast audio-video signals (column 7, lines 5-14: *a smart card for decrypting video transmissions*).

Claim 16 is rejected as applied above in rejecting claim 2. Furthermore, Bowman discloses:

The semiconductor integrated circuit according to claim 2 wherein the at least one of the one or more hardware circuit portions relates to storing audio-video signals to an external storage device, whereby the enabling circuit is arranged to selectively restrict, deny, or allow storage of the audio-video signals produced by the circuit (column 7, lines 5-27).

Claim 17 is rejected as applied above in rejecting claim 2. Furthermore, Bowman teaches:

The semiconductor integrated circuit according to claim 2 comprising an input for receiving broadcast signals from a broadcast network from which the audio-video signals are produced, and wherein the at least one of the one or more hardware circuit portions relates to production of the audio-video signals (column 7, lines 5-14: *a smart card for decrypting video transmissions*).

However, Bowman does not explicitly state that the enabling circuit is arranged to selectively, restrict, deny, or allow the production of the audio-video signals. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Regarding claim 18, Bowman discloses:

A television decoder comprising:

a semiconductor integrated circuit that comprises an input interface for receipt of a received encrypted enable signal (column 2, lines 26-30: *authorized receiver receives an encrypted signal*);

an output interface for output of audio-video signals (Fig. 4b: *step AJ: outputs decrypted information*);

one or more hardware circuit portions each arranged to process data in relation to the audio-video signals (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*);

a decryption circuit arranged to receive the encrypted enable signal and to decrypt the encrypted enable signal in accordance with a key to provide a plain text message (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*);

a store containing a stored value for the circuit (column 7, lines 18-27: *the memory stores at least two pre-defined constants used to derive the decryption key*).

a second decryption circuit in one or more hardware circuit portions and arranged to receive a common key from a common key store in the integrated circuit and to decrypt the received encrypted broadcast signal in response to receipt of the common key and the generation of the enable signal (column 6, lines 40-55: *wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly teach an enabling circuit to selectively restrict, deny or allow operation of a hardware circuit portion and a comparison circuit to compare the plain text message to the stored value to instruct the enabling device. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Regarding claim 19, Bowman discloses:

A method of providing an audio video device to a user, the audio video device of the type for manipulation and presentation of audio video content and comprising a plurality of hardware circuit portions on a monolithic semiconductor circuit, and an input interface, the method comprising:

supplying the audio video device for an end user in a condition that one or more of the hardware circuit portions are inoperable or have reduced functionality (column 1, lines 15-30, column 7, lines 5-17: *satellite television applications, wherein the receiver needs the correct key to be able to decrypt the transmissions*);

arranging a subscription agreement with the end user in which the user pays for ongoing functionality of the one or more hardware circuit portions (column 1, lines 15-30: *satellite television applications*).

Bowman does not explicitly disclose providing an enable message in encrypted form for input to the input interface, the enable message instructing the monolithic semiconductor circuit to enable functionality of one of the one or more hardware circuit portions. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 20 is rejected as applied above in rejecting claim 19. Furthermore, Bowman discloses:

The method according to claim 19 wherein the audio-video device is a television decoder (column 1, lines 15-30: *satellite television applications*).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Bowman discloses:

The method according to claim 20 wherein the enable message is broadcast to the audio-video device (column 1, lines 15-30: *satellite television applications*).

Claim 22 is rejected as applied above in rejecting claim 20. Furthermore, Bowman discloses:

The method according to claim 20 wherein one of the plurality of hardware circuit portions is a cryptographic processor for decryption of television signals (column 1, lines 15-30).

Bowman does not explicitly disclose that the enable message the instructing the enablement of the cryptographic processor. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 23 is rejected as applied above in rejecting claim 20. Furthermore, Johnson discloses:

The method according to claim 20 wherein one of the plurality of hardware circuit portions is a data port, the enable message instructing the connection or disconnection of the data port (column 6, lines 10-42).

Regarding claim 24, Bowman discloses:

A circuit, comprising:

a decryption circuit adapted to decrypt an encrypted enable signal in accordance with a key to output a plain text message (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*).

a second decryption circuit adapted to decrypt the encrypted broadcast signals and produce the audio-video signals in response to receipt of a pre-stored common key and the control signal (column 6, lines 40-55: *wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly disclose a comparison circuit adapted to compare the plain text message with a stored value and selectively output a control signal if the plain text message matches the stored value. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Johnson discloses:

The circuit of claim 24, comprising an enabling circuit adapted to selectively enable, disable, and restrict operation of at least one other circuit in response to the control signal (column 6, lines 10-42).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Johnson discloses:

The circuit of claim 25, wherein the enable circuit is adapted to select which of a plurality of other circuits to selectively enable, disable, and restrict operation in response to the control signal (column 6, lines 10-42).

Regarding claim 27, Bowman discloses:

A method of controlling a circuit, comprising:

decrypting an encrypted enable signal in accordance with a key to output a plain text message (column 7, lines 5-17: *receives encrypted transmission and decrypts the transmission*).

decrypting the encrypted broadcast signals and produce the audio-video signals in response to receipt of a pre-stored common key and the control signal (column 6, lines 40-55: *wherein the s-key values is provided to a receiver from a data table*).

Bowman does not explicitly disclose comparing the plain text message with a stored value and selectively outputting a control signal if the plain text message matches the stored value. Johnson, in an analogous art, discloses comparing a stored key against a received decrypted key, and if they match, the comparator sends an enable signal to a multiplexer (Johnson: column 6, lines 10-20). It would have been obvious to one of ordinary skill in the art to implement the enabling circuit of Johnson into the system of Bowman in order to secure the system from attack by an unauthorized party (Johnson: column 3, lines 50-55).

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Johnson discloses:

The method of claim 27, comprising the further step of selectively enabling, disabling, and restricting operation of at least one other circuit in response to the control signal (column 6, lines 10-42).

Claim 29 is rejected as applied above in rejecting claim 28. Furthermore, Johnson discloses:

The method of claim 28, wherein selectively enabling, disabling, and restricting operation comprises selecting which of a plurality of other circuits to selectively enable, disable, and restrict operation in response to the control signal (column 6, lines 10-42).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
01/29/2010
Primary Examiner, Art Unit 2431